Getting Started For Terminal Operations

SECURITY MANAGEMENT

Security Management refers to the maintenance of user profiles, including the resetting of password. Each Participant is required to assign at least two Delegated Administrators (DA) to manage the basic security profile of his/her CCMS users (e.g., change user name, assign user groups to individual users, etc.). The two DAs, acting as maker and checker respectively, will receive different smartcards with different user IDs to perform their responsible functions. Please refer to table 3.2.1 for the full list of security functions.

To appoint and cancel the assignment of a DA, a Participant must complete and submit to the Clearing House the form 'User Profile for Delegated Administrator (DA)'. Upon receipt of the valid form, the Clearing House will provide to the Participant concerned a unique User ID and smartcard for the DA. The Participant must ensure that its DA creates or changes his initial Smartcard Password (where applicable) immediately upon receipt of the smartcard. Please refer to Section 3.3 for detail procedures.

The Security Management functions are accessible via a separate URL ***https://www.ccass.com/dms***. The logon procedures for the Security Management are basically the same as those for accessing other CCMS functions, except that users should type ***https://www.ccass.com/dms*** instead of the CCMS/CCASS URL in the box next to the address field when they logon to the security management functions. Please refer to Section 3.4 for the detailed logon procedures.

Table 3.2.1 lists the functions and reports related to Security Management transactions.

TABLE 3.2.1: Functions and reports related to Security Management transactions

	Functions	Section in this User Guide
Terminal operation functions	• User Profile Maintenance • Get Authorisation Code • Reset smartcard password	Section 7.2.1 Section 7.2.8 Section7.2.7
Reports	• User Group Listing (with Accessible C/3 Functions) • User Profile Listing • Disabled User Listing • SRN Listing • User Profile Maintenance Report	Section 7.2.2 Section 7.2.3 Section 7.2.4 Section 7.2.5 Section 7.2.6

Table 3.2.2 summarises the administration rights that can be assigned to the DAs regarding the Security Management functions to be performed by Participants.

TABLE 3.2.2: Administration rights related to Security Management transactions

Administration Rights	**Function**	**Remarks**
Maintain User Profile	• Change User Profile Input / modify user name, input transaction limits and user groups; enable or disable a user	Maker-checker mechanism is provided.
	• Delete User Profile	
	• Enquire User Profile	
	• Get Authorisation Code	For enquiry of the authorisation code by checker.
	View Listings • User Group Listing (With Accessible C/3 Functions) • User Profile Listing • Disabled User Listing • SRN Listing #	
	View Report • User Profile Maintenance Report	
Reset Smartcard Password	• Reset smartcard password Smartcard password of authorised users only; not applicable to smartcard password of DA, which will be reset by HKEX	• No maker-checker mechanism. • Can be a separate function performed by a different DA.
	• Enquire User Profile	
	View Listings • User Group Listing (With Accessible C/3 Functions) • User Profile Listing • Disabled User Listing • SRN Listing #	
	View Report • User Profile Maintenance Report	

A List of the 'Subscriber Reference Number' encrypted in each smartcard issued to users and DA.